The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB GOVERNMENT'S MOTION FOR RECONSIDERATION OF ORDER GRANTING DEFENDANT'S THIRD MOTION TO COMPEL AND FOR LEAVE TO SUBMIT RULE 16(d)(1) FILING *EX PARTE* AND *IN CAMERA* [redacted] ***Noting Date: April 8, 2016***

I. INTRODUCTION

With this motion, the United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Helen J. Brunner, Michael Dion, Andre M. Penalver, and Matthew P. Hampton, Assistant United States Attorneys for said District, and Keith A. Becker, Trial Attorney, takes the unusual step of requesting this Court to reconsider its Order Granting Defendant's Third Motion to Compel Discovery (Dkt. 161). [redacted]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

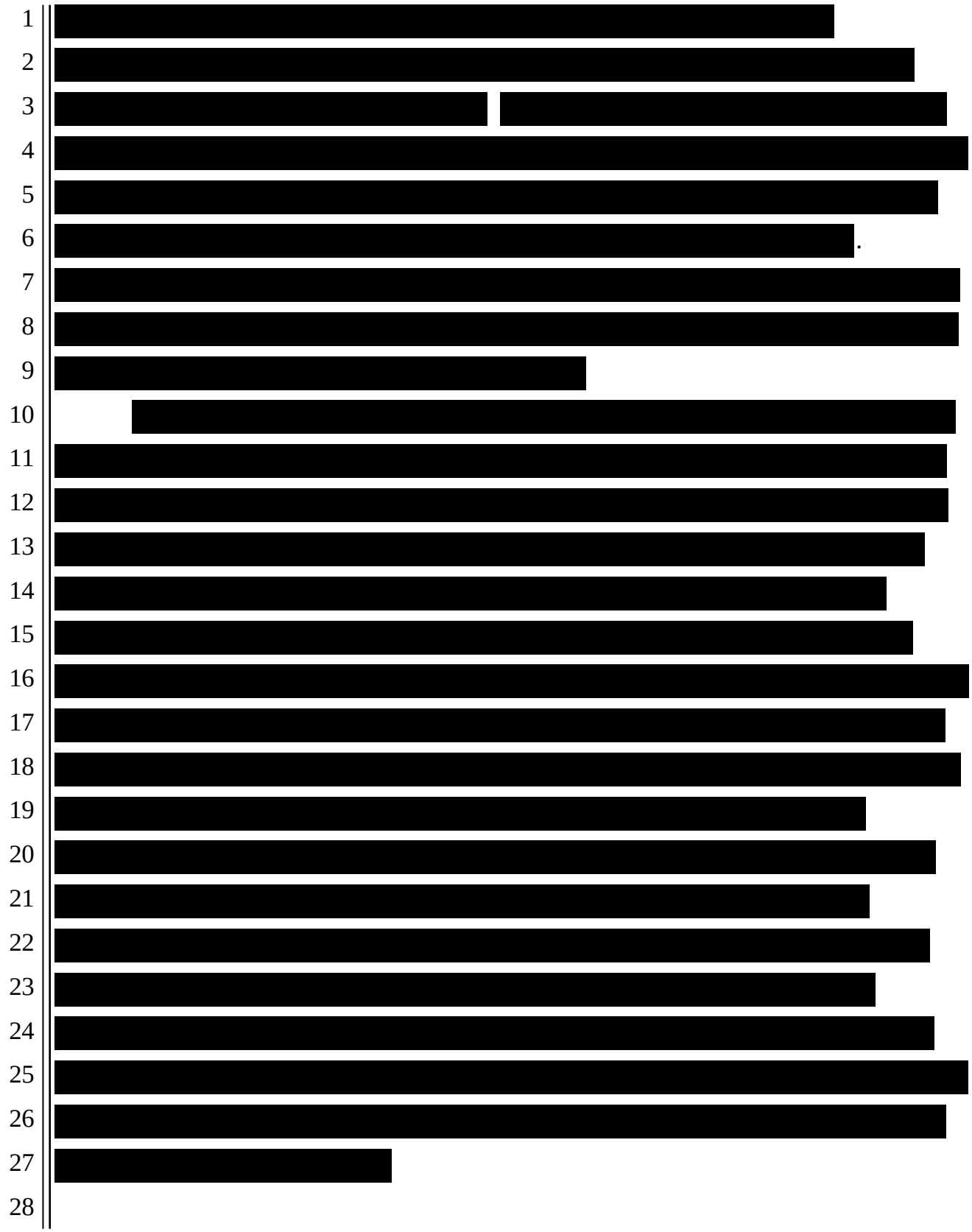
[redacted]

For these and the other reasons outlined below, the United States is now taking the unusual step of asking this Court to reconsider its Order. The substance of this motion outlines the government's reasoning for why the information the Court ordered the government to disclose does not actually answer the questions the defense claims it needs this information to answer. [redacted]

II. ARGUMENT

[redacted]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800



UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Because the *ex parte* filing will not be available to the defense, we have included the broad outlines of the concerns here to provide the defense with notice. The primary focus of this memorandum is to address in greater detail the reasons why the lack of access to what the defense expert refers to as the "exploit" and the other desired information will not deprive the defense of the ability to address the concerns expressed in the defense pleadings and therefore why reconsideration is appropriate on this basis as well. Those issues will not be addressed in the *ex parte* filing. The accompanying declaration of FBI Special Agent Daniel Alfin provides factual details to support the government's claims.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

B. The Information the Court Ordered the Government to Disclose Will Not Address the Defense's Stated Concerns.

Evaluation of the discovery requested by the defense must begin with consideration of the evidence obtained both through the deployment of the computer code that the government considers the NIT on Michaud's computer,[1] and through the subsequent execution of a search warrant at Michaud's residence.

As detailed previously, the NIT warrant authorized the collection of discrete information from target computers, including an IP address, a MAC address, and information related to the operating system and user account. In this case, the information obtained through the deployment of the NIT to the computer used by Playpen user "pewter" resulted in the execution of a search warrant at Michaud's home and his arrest. From his home, agents seized, among other things, Michaud's personal computer, two thumb drives used as electronic storage devices, and another computer that belonged to Michaud's employer. In addition, agents seized Michaud's cell phone incident to his arrest. Subsequent forensic examination of the cell phone and the two thumb drives—one of which was plugged into Michaud's television at the time of the search—confirmed those devices contained images/videos of child pornography and child erotica. Some of the images had been curated and organized into folders by subject. For example, one of those thumb drives contained a folder entitled "downloads" with dozens of subfolders with names such as "Little-Virgins" and "Nasties" that contained child pornography and child erotica. The evidence found on these thumb drives and Michaud's cell phone form the basis for Counts 1 and 3 of the Superseding Indictment.

[1] Although the defense chooses to define the NIT to include every aspect of obtaining information from the computers connecting to Playpen as a result of the Eastern District of Virginia warrant, the United States has not characterized the term as such. Indeed, that is obvious from the Eastern District of Virginia warrant. A warrant is required for a Fourth Amendment intrusion. Thus, for purposes of issuance of a warrant, except for night time execution or whether the agents may execute without knocking, it is irrelevant if the agents travel to or even how they gain entry to a residence to execute a warrant. What was authorized by the Eastern District of Virginia warrant was deployment of computer code (or NIT) on computer or other devices connecting to Playpen, in order to obtain the IP addresses and other information necessary to identify the user.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Count 2, charging Michaud with receipt of child pornography, pertains to his use of Playpen during the period when it was under FBI control.

Michaud articulated two reasons to justify his request for discovery of the method of deployment of the NIT to Michaud's computer, and the method by which the government captured the data retrieved as a result of the NIT. Those reasons can be summarized as follows: (1) to verify the accuracy of the information collected and ensure that the NIT did not exceed the scope of the authorizing warrant; and (2) to evaluate the merits of defense theory that someone or something else is responsible for the child pornography found on his devices. These reasons, however, do not establish the need for this discovery. Indeed, the defense expert's declaration does little more than saying it is so. Thus, the government now asks this Court to reconsider that basis for the Order as well.

Michaud's claim that he needs additional discovery to verify the accuracy of the information collected by the NIT and confirm that the agents did not exceed the scope of the warrant authorizing the deployment of the NIT is not supported even by his expert's claims. To the contrary, Michaud has everything he needs to do this analysis. As this Court is aware, the government provided the defense expert with access to the computer code that actually performed the "search" of Michaud's computer, as well as the results of that search. The government even offered to provide (and Michaud has so far declined to review) the network data stream showing the communication between Michaud's computer and the government computer during the execution of the NIT. The government has reviewed that data stream, however. *See* Declaration of Special Agent Daniel Alfin in Support of Government's Motion for Reconsideration (Alfin Decl.) ¶¶ 11-15. As Agent Alfin explains, reviewing the packets of information exchanged by Michaud's computer and the government computer demonstrates that the specific information that the government recorded *receiving* from Michaud's computer is in fact the specific information that Michaud's computer *sent* to the government. *Id.* Of the nine network packets comprising the data stream, eight reflect information necessary for

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

ordinary network traffic over the Internet. The remaining packet contains the substance of the communication of the NIT results from Michaud's computer—the substance that is identical to what was stored on the government's servers as having been received from Michaud's computer. *Id.*

Nor do Michaud's individual requests withstand scrutiny under his logic. Discovery about what Michaud's expert has referred to as the "exploit" would undoubtedly shed light on how the NIT actually was delivered to his computer. But it would offer no information about what the NIT did on Michaud's computer and what information was collected as a result of its deployment. Alfin Decl. ¶ 7. His claimed need for information about the servers on which the NIT results were stored is similarly unavailing. Any concern about corruption or other errors that might cast doubt on the accuracy of the information obtained through the NIT instruction that is associated with Michaud's computer can be addressed by review of the information that *was actually collected*. Alfin Decl. ¶¶ 11-15.

Finally, the suggestion that there might be some error in the creation of the unique identifiers used to track the NIT results from individual computers to which it was deployed, does not demonstrate the need to know the manner in which the NIT instructions were delivered. Although there is a theoretical possibility of a problem with unique identifiers, the government has confirmed that the unique identifiers associated with the NIT results for Michaud's computer—just like the other unique identifiers for the other targets of the NIT—were in fact unique. Alfin Decl. ¶¶ 8-10.

Moreover, even if there were something to Michaud's concerns above, those concerns relate only to the question of whether there was probable cause to support the warrant authorizing the search of his home. And unless any such defects were obvious, the warrant would still stand, since the IP address directly tied to Michaud's residence, and the evidence seized as a result—including the thumb drives and the cellular phone containing child pornography—could still be used to support Counts 1 and 3 of the

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Superseding Indictment—which are premised not on Michaud's activity using Playpen but rather the evidence seized from his home.

Michaud also says that the additional discovery is necessary because someone or something else could be responsible for planting the thousands of images of child pornography found on his electronic storage devices. Other than identifying this as a theoretical possibility, however, Michaud points to no factual support for his claim that further discovery regarding the NIT would be helpful in developing that theory, something that seems particularly problematic in light of the organized treatment of this material on the thumb drives.

Indeed, despite having access to the devices themselves, their contents, and the NIT computer instructions, Michaud identifies not a scintilla of evidence to support his theory. He has not even, so far as the government is aware, attempted to examine the devices in the government's custody. Yet he insists that further discovery related to the method of deployment of the NIT is critical to evaluating the potential viability of this theory. The defense's speculation may be plausible in theory but completely collapses when one considers the actual evidence found in this case.

After all, none of the devices on which child pornography was found (Michaud's two thumb-drives and his cellular phone) were the actual target of the NIT. Michaud thus cannot credibly claim that additional discovery related to the NIT would somehow bear on how this extensive collection of child pornography found its way on those devices in the extremely organized fashion in which it was arranged. It would not, for example, shed light on who plugged one of those thumb drives into the back of Michaud's television or who organized the contents of the "downloads" folder described above. Nor would it help explain how a phone containing child pornography was in Michaud's possession at the time of his arrest. Were there anything at all to his theory, Michaud would surely point to something in the devices or their contents that lends credence or explain why he cannot. In the end, he offers little more than *hope* the information he

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

seeks will somehow aid his cause. All he has argued is simply that a thumb drive can be connected to a computer.

Indeed, the one device to which the NIT was likely deployed, Michaud's personal computer, is a device on which no child pornography was found. This is not surprising because someone, presumably Michaud, reset that computer to a preset configuration and erased the hard drive the night before the search warrant was executed. Regardless, Michaud and his expert have access to this computer and a forensic image of its hard drive to analyze. And here too, Michaud offers nothing to support his theory that the requested information will somehow bolster his baseless claim that the method of deploying the net NIT somehow opened the door for some nefarious entity to place thousands of images of child pornography on his devices.

Even Michaud's own expert declaration does not support his claimed need. While Michaud has at various times suggested that the NIT computer instructions "alter," "compromise," or "override" security features on a user's computer, Reply (Dkt. 149) at 2-3, 5-6, nothing in his expert's declaration supports such a claim. The words "alter" and "override" appear nowhere in the Tsyrklevich declaration. Dkt. 115-1. And the word "compromise" appears only in the context of what defense counsel told him: "defense counsel has informed me that he is seeking to determine . . . whether [the NIT's] execution may have compromised any data or functions on the target computer." *Id*. at 3. What Mr. Tsyrklevich does say is that an "exploit," consists of software that "takes advantage of a software 'vulnerability' in the Tor Browser program" and that "the NIT is able to circumvent the security protections in the Tor Browser." Dkt. 115-1 at 2. He goes on to explain he needs to examine the "exploit" component to understand "whether the payload data that has been provided in discovery was the only component executing and reporting information to the government or whether the exploit executed additional functions outside of the scope of the NIT warrant." Dkt. 115-1 at 3. But what he refers to as the "payload data" has been provided in discovery. The government has confirmed that this was the only "payload"—as Michaud defines it—sent to Michaud's computer.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Declaration of FBI Special Agent Daniel Alfin in Support of Governments Surreply to Defendant's Third Motion to Compel (Dkt. 157) ¶ 5. Nowhere in the Tsyrklevich declaration does it state that it is possible that any of the other components related to the use of the NIT could have planted child pornography on Michaud's computer or left the computer vulnerable to some other "virus" or "remote user" capable of doing so.[2]

In the end, none of the questions Michaud claims need to be answered will actually be answered by the discovery he seeks. If he wishes to verify the accuracy of the NIT information or the scope of the NIT search, then he should look to the NIT code already in his possession and the information collected by the NIT. And if he wishes to test the viability of a "someone-else-did-it" theory, then he should look to the actual evidence of the charged crimes—his devices—for those answers. He has what he needs to answer the questions he has raised, and additional discovery related to the NIT will be of no use in that endeavor.

III. CONCLUSION

For the reasons, set forth above, the government respectfully asks this Court to reconsider its Order. As detailed above, the government continues to maintain that Michaud has all the necessary tools to verify the NIT data and confirm that the NIT operated as the government has said it did. His justifications for the requested discovery rest on speculation, not fact, and he has made no showing that would support the requested discovery. To the extent that this Court agrees with this assertion, this Court may grant the motion to reconsider without the need to consider or address the government's proposed *ex parte* filing. Should the Court continue to find that the information sought is somehow material, it may nevertheless "deny" production of that

---

[2] The court also addressed the issue of whether the NIT provided further access to Michaud's computer during the January 22, 2016, suppression hearing – asking Special Agent Alfin whether there was "any way for the FBI to go back down this NIT to get into the subject computer, the user's computer?" Jan. 22, 2016, Tr. p. 71. SA Alfin answered, "[n]o, your Honor. After the NIT collected the limited amount of information that it was permitted to collect, there was nothing that resided on the subject's computer that would allow the government to go back and further access that computer." Id., p. 71-72. The Court credited Special Agent Alfin's testimony.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

information for "good cause" pursuant to Rule 16(d)(1). Accordingly, the United States would ask the Court [redacted] to reconsider its order.

DATED this 28th day of March, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
HELEN J. BRUNNER
MICHAEL DION
ANDRE M. PENALVER
MATTHEW P. HAMPTON
Assistants United States Attorney
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Telephone: (206) 553-7970
Fax: (206) 553-0755
E-mail: matthew.hampton@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on March 28, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant(s).

s/Emily Miller
EMILY MILLER
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-2267
FAX: (206) 553-0755
E-mail: emily.miller@usdoj.gov